Allied Telesis™

AT-S63 Version 4.0.0 Patch 2 Management Software for the AT-9400 Basic Layer 3 Gigabit Ethernet Switches Software Release Notes

Please read this document before you begin to use the management software.

Included in this document are the following:

- ❐ “Supported Platforms” on page 2
- ❐ “Product Documentation” on page 3
- ❐ “Switch Models and Management Software” on page 3
- ❐ “New and Enhanced Version 4.0.0 Features” on page 3
- ❐ “Upgrading Stand-alone AT-9400 Switches” on page 5
- ❐ “Upgrading AT-9400 Stacks” on page 6
- ❐ “AT-9424T Switch” on page 7
- ❐ “Stacking Tips” on page 7
- ❐ “Version 4.0.0 Known Issues” on page 8
- ❐ “Version 4.0.0 Patch 2 Resolved Issues” on page 9
- ❐ “Version 4.0.0 Resolved Issues” on page 9
- ❐ “Version 4.0.0 Operational Notes” on page 10
- ❐ “Features History” on page 14
- ❐ “Contacting Allied Telesis” on page 19

Supported Platforms

AT-S63 Version 4.0.0 Management Software is supported on the following AT-9400 Gigabit Ethernet Switches:

Basic Layer 3 Models	AT-9424T (AC)
	AT-9424T/POE (AC)
	AT-9424Ts (AC)
	AT-9424Ts/XP (AC)
	AT-9448T/SP (AC)
	AT-9448Ts/XP (AC)

Note:
AT-9400 Basic Layer 3 Switches that have Version 2.1.0 or earlier of the AT-S63 Management Software must be upgraded to Version 2.2.0 before they are upgraded to Version 4.0.0. For the Internet locations of the management software for Allied Telesis products, refer to “Management Software Updates” on page 19.

This release supports the following redundant power supply on the AC models:

❒ AT-RPS3204

For a list of supported GBIC, SFP, and XFP modules, contact your Allied Telesis sales representative.

This version does not support the following AT-9400 Switches:

Layer 2+ Models	AT-9408LC/SP (AC)
	AT-9424T/GB (AC)
	AT-9424T/SP (AC)
	AT-9424T/GB-80 (DC)
	AT-9424T/SP-80 (DC)

Caution:
The software described in the documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a “retail encryption item” in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product’s export status.

Product Documentation

Refer to the Allied Telesis web site at **www.alliedtelesis.com** for the latest installation and user guides.

Switch Models and Management Software

The following table lists the models in the AT-9400 Series and the versions numbers of the AT-S63 Management Software when they were initially supported. If you want to load an older version of the management software onto a switch, you should refer to the table to determine whether the version supports the switch. For example, support for the AT-9424Ts Switch was introduced in version 2.1.1. Any attempt to load an earlier version of the software on that model will be unsuccessful.

Model	AT-S63 Management Software Version
AT-9424T/GB	1.0.0
AT-9424T/SP	1.0.0
AT-9408LC/SP	1.1.0
AT-9448Ts/XP	1.3.0
AT-9448T/SP	2.0.0
AT-9424Ts/XP	2.0.0
AT-9424Ts	2.1.1
AT-9424T (version 1)	3.1.0
AT-9424T/POE	3.2.0
AT-9424T (version 2)	4.0.0

New and Enhanced Version 4.0.0 Features

Stand-alone AT-9400 Switches

Here are the new and enhanced features in AT-S63 Management Software for stand-alone switches:

- ❒ Stand-alone switches now support up to three manager sessions at one time. To adjust this feature, which has a default setting of one manager session, use the SET SYSTEM command.
- ❒ The 802.1x port-based network access control feature is now fully compliant with the following:
  - — Microsoft Network Access Protocol on Windows Server 2008, Windows Vista, and Windows XP Service Pack 3
  - — Symantec Network Access Control

- The management software has a new command line interface based on the commands in the AlliedWare Plus™ operating system found on other Allied Telesis products, such as the Layer 3 switches. If you are already familiar with the commands in the AlliedWare Plus™ operating system, you may find this new interface more convenient to use than the standard command line. Some of the management functions you can perform with this new interface are:
  - Configure port parameters, such as Auto-Negotiation, speed, and duplex mode
  - Create new tagged and untagged VLANs
  - Create access control lists and Quality of Service policies
  - Create routing interfaces
  - View the MAC address table and add static addresses

Note:
This version of the AT-S63 Management Software supports only a limited number of AlliedWare Plus™ commands. For further information, refer to the latest version of the *AT-S63 Management Software Command Line Interface User's Guide*.

AT-9400 Stacks

Here are the new and enhanced features in AT-S63 Management Software for AT-9400 Stacks:

- BOOTP/DHCP Relay Agent
- Access Control Lists
- Quality of Service policies
- IPv4 static routes
- Encrypted remote web browser management sessions with the Secure Sockets Layer protocol and the Public Key Infrastructure protocol
- Encrypted remote Secure Shell protocol management sessions
- AlliedWare Plus™ Command Line Interface. For a description, refer to "Stand-alone AT-9400 Switches" on page 3.
- Stacks now support up to three manager sessions at one time. To adjust this feature, which has a default setting of one manager session, use the SET SYSTEM command.
- The LOAD command in the standard command line interface has a new parameter that will make it easier in future releases of the AT-S63 Management Software to update the AT-9400 Switches of a stack. In previous versions, you had to disassemble a stack and update the switches individually. But with the new MODULE parameter, you'll be able to update the management software on all the switches in a stack simultaneously.

Note:
The new MODULE parameter can only be used on stacks that already have Version 4.0.0 or later. To update member switches that have versions earlier than 4.0.0, you have to disconnect them from the stack and update them as stand-alone units.

- The 802.1x port-based network access control feature is now fully compliant with the following:
  - Microsoft Network Access Protocol on Windows Server 2008, Windows Vista, and Windows XP Service Pack 3
  - Symantec Network Access Control
- The commands used to control the MAC address table have a new MODULE parameter that lets you manage the MAC address tables on the individual switches of a stack.
- Switches assigned static ID numbers continue to use stack configuration files even when the stack stops operating and the switches revert to stand-alone units. This feature enables the switches to retain their stack configuration settings as stand-alone units, which may lessen the impact to network operations if the stack encounters a problem. For more information, refer to the latest version of the *AT-S63 Management Software Features Guide*.

Upgrading Stand-alone AT-9400 Switches

You can upgrade a stand-alone switch from a local management session with either XMODEM or TFTP, or from a remote Telnet, SSH, or web browser session with TFTP. For instructions, refer to the AT-S63 documentation set.

After you have upgraded the management software on a stand-alone switch, you need to check its stack ID number. Starting in Version 4.0.0 stand-alone switches that have a static ID number use the stack configuration file instead of the stand-alone configuration file as their active configuration file. In previous versions, the stack configuration file was used only when a switch detected that it was a master switch or a backup master switch of a stack. The purpose of this change is to make it possible for a master switch and a backup master switch to maintain their stack configuration settings if the switches revert to stand-alone units should a stack encounter a problem.

When a stand-alone switch that has a static ID number is upgraded to Version 4.0.0, it uses the stack configuration file instead of the stand-alone file after it resets. This may give the impression that it has lost all of its configuration settings. To remedy this, you must change the stack ID number assignment from static to automatic. Stand-alone switches that have an automatic stack ID assignment always use the stand-alone configuration file.

To check the switch's stack ID number:

1. Log on the switch as the manager.
2. Enter the following command to display the switch's current stack ID number:

   ```
   show stack
   ```

   Here is an example of the information:

   ```
   Local MAC Addr              :00:30:84:00:00:03
   Standalone Mode ID          :1
   Stack Mode                  :AUTO
   Stack ID                    :1
   Stack Priority              :16
   ```

3. If the Stack Mode parameter is AUTO, you are finished updating the stand-alone switch. However, if it is set to STATIC, you need to change the Stack Mode to automatic with this command:

   ```
   set stack moduleid=n newmoduleid=auto
   ```

The variable *n* is the current value of the Stack ID parameter in the display. For example, if the current value of the parameter is 1, the command would be:

```
set stack moduleid=1 newmoduleid=auto
```

4. After entering the command, you need to reset the switch with this command because your change to the switch's ID assignment does not take affect until the unit is reset:

```
restart reboot
```

5. After the switch has completed the reset, log on again as the manager.
6. Enter this command again:

```
show stack
```

7. Verify that the Stack Mode is now AUTO. If it is, then you are finished updating the stand-alone switch. If it is still STATIC, try repeating the command in step 3 and reset the unit.

Upgrading AT-9400 Stacks

The switches of a stack have to be upgraded as stand-alone units. This requires removing the stacking cables from the switches. (In future releases, you'll be able to use the new MODULE parameter in the LOAD command and update the switches all at the same time.) To upgrade the management software on the switches of a stack:

1. Start a local or remote management session on the master switch of the stack.
2. Enter the SAVE CONFIGURATION command to save the stack's current configuration.
3. Enter LOGOUT to end the management session.
4. Power off the switches of the stack.
5. Disconnect the stacking cables from the AT-StackXG Modules.
6. Power on one of the switches and establish a local management session.
7. Download the new management software using XMODEM or TFTP. The command to download the new software with XMODEM is:

```
load method=xmodem destfile=appblock
```

For instructions on how to download the new software using TFTP, refer to the AT-S63 documentation set.

8. After upgrading the management software on the switch, end the management session and power off the switch.
9. Repeat steps 6, 7, and 8 on each of the switches in the stack.
10. After upgrading all the stack units, reconnect the stacking cables to the AT-StackXG Modules.
11. Power on the switches. The switches can be powered on in any order.

Note:
All the switches in a stack must use the same version of the AT-S63 Management Software. Otherwise, the stack may not successfully form and/or experience performance problems.

AT-9424T Switch

AT-9424T Switches shipped after March 2009 and having “04221” in their serial numbers must use Version 4.0.0 or later of the AT-S63 Management Software. Downloading earlier versions of the management software onto these switches causes them to fail during bootup.

Serial Number - x04221xxxxxxxxxx

Stacking Tips

❒ Stack Size

The maximum number of switches in a stack varies according to the switch model. A stack can have up to eight units of AT-9424Ts Switches, AT-9424Ts/XP Switches or a combination of both.

Stacks can also have the AT-9448Ts/XP Switch, but Allied Telesis does not recommend using this model as a master switch. Consequently, a stack with one or more of these switches should have an AT-9424Ts or AT-9424Ts/XP Switch acting as the master switch. For stacks of more than three switches, both the master switch and the backup switch should be 24-port switches. A stack should not have more than four AT-9448Ts/XP Switches and should not exceed a total of eight units, as shown in this table.

		Number of 24-Port AT-9424Ts and AT-9424Ts/XP Switches								
Number of 48-Port AT-9448Ts/XP Switches		0	1	2	3	4	5	6	7	8
	0		■	■	■	■	■	■	■	■
	1	■	■	■	■	■	■	■	■	
	2	■	■	■	■	■	■	■		
	3			■	■	■	■			
	4			■	■	■				

❒ Adding switches to a stack. To add a switch to an existing stack, follow this procedure. (The references are to Chapter 3, “Preparing the Switches of a Stack,” in the *AT-9400 Stack Installation Guide*.)

1. Install the AT-StackXG Module in the switch. For instructions, refer to the Installation Guide included with the module or Chapter 2, Installing the Hardware, in the *AT-9400 Stack Installation Guide*.
2. Verify that the new switch has the same version of the AT-S63 Management Software as the other stack members. For instructions, refer to “Verifying the AT-S63 Version Numbers.” If necessary, upgrade the unit’s software.
3. Assign the switch a static module ID number by performing the instructions in “Assigning Status Module ID Numbers to the Member Switches.”
4. This step is optional. If you assigned the switch a stack ID number greater than 2, you might want to consider configuring its parameter settings to match as closely as possible its likely configuration when it is a part of the stack. Although the stand-alone configuration of a switch is not transferred to its operations as a member of a stack, configuring the switch for both stand-alone and stack operations might mitigate the impact

on the operations of your network in the event the stack stops functioning. This is because the switches that comprise a stack automatically revert to stand-alone operations if a stack experiences a problem. (This isn’t necessary for a switch assigned the stack ID 1 or 2 because it uses the stack configuration file for both stack and stand-alone operations.)

5. Power off the switch.
6. Cable the switch to the other switches in the stack as explained in “Cabling the AT-StackXG Stacking Modules.”
7. To monitor the progress of the discovery process, connect a terminal to the Terminal Port on the master switch.
8. Log in and configure the parameter settings on the new member of the stack.
9. To add additional members to the stack, repeat this procedure. You should add only one switch at a time to an stack and should verify that the stack is functioning properly before adding another switch.

Note:
Adding or removing members from a stack will be disruptive to the operations of your network because the switches do not forward traffic during the discovery process.

❐ 802.1x port-based network access control. A stack does not support MAC address-based authentication.

❐ Stack table sizes. The sizes of the MAC, ARP, and VLAN tables in a stack are:

— 16k MAC Addresses

— 2k ARP Entries

— 4094 VLANs

Version 4.0.0 Known Issues

❐ Slow Management Sessions with Large Stack - Remote Telnet, SSH, and web browser management sessions may be slow when a stack has a large number of switches and when the remote management station is communicating with a stack through a member switch rather than a master switch. To avoid this problem, try to conduct your remote management sessions from remote workstations that are communicating directly with a master switch. This issue affects management traffic only and does not affect the switching or the routing functions of a stack.

❐ Enhanced Stacking Through the Web Browser Windows. The enhanced stacking feature is not supported through the web browser windows on the AT-9424Ts, AT-9424Ts/XP, and AT-9448Ts/XP Switches, but is supported through the standard command line interface and the menus. (5871, 6467)

❐ SNTP Settings. The switch does not retain the SNTP settings. You have to reenter the settings when you reset or power cycle the unit. (6475)

❐ 802.1x Control Direction parameter. The Control Direction parameter for 802.1x authenticator ports has an Ingress option for forwarding egress broadcast and multicast traffic when the ports are in the unauthorized state. This option is nonfunctional and instead blocks these packets. (5487)

Version 4.0.0 Patch 2 Resolved Issues

The following issues were resolved in Version 4.0.0 Patch 2 of the AT-S63 Management Software:

- ❐ Default Route. If there was a change to the path of the default route on an AT-9400 Stack, the nodes connected to the stack would lose connectivity to the remote destinations of the route until they issue a new ARP.
- ❐ ARP Table Entries - The AT-9424Ts, AT-9424Ts/XP and AT-9448Ts/XP Switches were not aging out entries from the ARP table.
- ❐ Master Switch and LACP - If there was a change in the composition of a stack and a new switch became the master switch, the previous master switch would continue to control the LACP processes, such as the task of designating the active ports in an aggregator, instead of relinquishing the role to the new master switch.

Version 4.0.0 Resolved Issues

The following issues were resolved in Version 4.0.0 of the AT-S63 Management Software:

- ❐ LACP - Stand-alone AT-9400 Switches and AT-9400 Stacks did not send LACPDUs on aggregators that had only one active link.
- ❐ Routing Link Aggregation - LACP trunks and static port trunks did not properly forward traffic from static routes or the default route.
- ❐ Tagged VLANs in Stacks - VLANs on AT-9400 Stacks did not always properly forward network traffic if they consisted of tagged ports on a master switch and untagged ports on member switches. (6605)
- ❐ ARP Requests on Tagged Ports of Member Switches - ARP requests that were received on the tagged ports on the member switches in an AT-9400 Stack were entered in the ARP table but were not replied to. (6606)
- ❐ Tagged Management Packets on the AT-9448Ts/XP Switch - Tagged management packets (e.g., ARP replies) received on ports 13 to 50 on the AT-9448Ts/XP Switch were replied to with untagged packets. (6497, 6614)
- ❐ Modifying VLANs Through Web Browser Windows - The management software would periodically fail when the VLANs were remotely managed with the web browser windows. (6747)
- ❐ ARP Timer - The ARP timer did not work, causing the switch to never age out entries from the ARP table. (5035)
- ❐ Character Limitation in the CREATE VLAN Command - The active boot configuration file of a stack would fail during the initialization process if the port numbers in a CREATE VLAN command exceeded 79 characters. (6711)
- ❐ Member Connected External Routes - Static routes and the default route only worked on the master switch of a stack. The routes did not work on member switches. (6362)
- ❐ SNMPv3 Walk - Performing an SNMPv3 walk on the switch would cause the management session to hang up because of a memory leak problem. (6416)
- ❐ SNMP Traps on Member Switches - The master switch of an AT-9400 Stack would not send SNMP traps from member switches after a stack topology change.

- ❐ Supplicant and VLAN Associations - The 802.1x port-based network access control feature could move a port to only one VLAN after receiving a VLAN association from a RADIUS server, and ignored future VLAN associations until a port was linked down and up again.
- ❐ PEAP and 802.1x Port-based Network Access - 802.1x Port-based Network Access now supports PEAP.

Version 4.0.0 Operational Notes

- ❐ Stacking and IGMP snooping. IGMP snooping on a stack requires that a multicaster be on a master switch.
- ❐ Web server. The default setting for the web server on the switch has been changed from enabled to disabled. To manage the switch with a web browser, enable the server with the ENABLE HTTP SERVER command.
- ❐ Classifier criteria. Access control lists and Quality of Service policies cannot filter on the following combinations of classifier criteria:

  — VLAN ID and source or destination IP address.

  — Protocol and source or destination IP address

  This rule applies whether the criteria are in the same classifier or in different classifiers that are applied to the same access control list or Quality of Service policy.
- ❐ Protocol (Layer 2) IP criterion - Do not use the IP value in the Protocol (Layer 2) variable of a classifier to filter IP traffic. The results may be unpredictable. Instead, use the IP source or the IP destination criterion. The following values can be used to filter large IP address ranges:

Value	Range
128.0.0.0/1	128.0.0.0 to 255.255.255.255
64.0.0.0/2	64.0.0.0 to 126.255.255.255
32.0.0.0/3	32.0.0.0 to 63.255.255.255
16.0.0.0/4	16.0.0.0 to 31.255.255.255
8.0.0.0/5	8.0.0.0 to 15.255.255.255
4.0.0.0/6	4.0.0.0 to 7.255.255.255
2.0.0.0/7	2.0.0.0 to 3.255.255.255
1.0.0.0/8	0 to 1.255.255.255

- ❐ ID numbers of ACLs. The ID numbers of permit ACLs have to be less than the ID numbers of deny ACLs. Otherwise, the results might be unpredictable on ports that have both permit and deny ACLs. To avoid this issue, start numbering your permit ACLs at ID number 1 and your deny ACLs at ID number 100.
- ❐ ID numbers of QoS policies. If you assign two QoS policies to the same port and one of the policies is filtering on a subset of the IP addresses of the other policy, the ID number of the subset policy has to be lower than the ID number of the other policy. Otherwise, the results might be unpredictable.

- ❐ Port Mirroring. In order for a switch to mirror tagged packets, the VLANs of the packets must exist on a switch. Packets that contain VIDs of nonexistent VLANs are not mirrored.
- ❐ Denial of Service defense mechanisms. The operation of a Denial or Service defense mechanism on the switch might be unpredictable when a defense is assigned to more than one port or when more than one defense is assigned to the same port. This issue can be avoided by not assigning a defense mechanism to more than one port or more than one defense mechanism to a port. This issue is limited to the AT-9424Ts and AT-9424Ts/XP switches. (4196)
- ❐ QoS policies and unicast and multicast addresses. The filtering properties of a QoS policy are designed for known unicast addresses. The behavior of a policy may be unpredictable if it filters on unknown unicast addresses or known or unknown multicast addresses. (3196)
- ❐ Lowest numbered port in an LACP aggregator. You cannot delete the lowest numbered port from an LACP aggregator, referred to as the base port, or add a port to an aggregator that is below the base port. The OperKey parameter for the ports in an aggregator is based on the lowest numbered port and cannot be changed after the aggregator is created. For example, if you create an aggregator of ports 10 to 15 on a switch, you cannot later delete port 10 from the aggregator or add a port less than port 10. You must recreate the aggregator if you need to change the base port. (4369)
- ❐ Saving a configuration. The management software on the switch may experience a problem if you save configuration changes in rapid succession. To avoid this issue, you should wait for the Fault LED on the front panel of the switch to go off after saving a configuration change and before saving another configuration change. If you are in a different location from the switch and cannot view the Fault LED, wait 30 to 45 seconds between your save commands. (2683)
- ❐ Multiple VLAN modes and IPv4 packet routing. The 802.1Q-compliant and non-802.1Q-compliant multiple VLAN modes do not support IPv4 packet routing. If you activate one of these modes, you cannot configure routing interfaces and all the existing routing interfaces, with the exception of the local interface, are deleted. To assign an IP address to a switch running one of these VLAN modes, you must create one routing interface and designate it as the local interface while the switch is running in the user-configured VLAN mode, and afterwards change the switch's VLAN mode to 802.1Q-compliant or non-802.1Q-compliant. The local interface is automatically moved to the VLAN on port 1. (3806)
- ❐ Switch to switch upload of a configuration file in an enhanced stack. The *AT-S63 Management Software User Guides* state that the routing interface commands in the configuration file on a master switch of an enhanced stack are retained when the file is uploaded to a slave switch. This is incorrect when the file being uploaded is the master switch's active configuration file. To prevent an IP address conflict on the units, the transfer automatically removes all routing interface commands as the active configuration file is uploaded. This rule only applies to the master switch's active configuration file. The transfer retains the routing interface definitions when you upload any other configuration file from a master switch to a slave switch. To avoid an IP address conflict in this situation, it may be necessary to modify the IP address assignments of the routing interfaces on the switch that received the file.(4272, 5873)
- ❐ Telnet management session. Changing the VLAN mode of a switch (e.g., from the user-configured VLAN mode to a multiple VLAN mode) from a remote Telnet management session may end your management session. To continue managing the switch, you must reestablish the management session (3806)

- ❒ AtiStkSwVlanConfigEntry MIB table. The response time of the management firmware on the switch will be slow if you have more than one instance of the AtiStkSwVlanConfigEntry MIB table open at a time. (2231)
- ❒ Compact flash card. Removing a compact flash card from the switch while the management software is writing a file to it may cause the switch to stop responding to management commands and forwarding network packets. To avoid this issue, never remove a compact flash card from the switch while the Fault LED on the front panel is on. Wait for the Fault LED to turn off before removing the card.(4253)
- ❒ LACP priority value and the event log. A change to a switch's LACP priority value is registered in the event log with a message that reflects the current status of LACP, rather than the change to the priority value. The log message is either "lacp:enabled" or "lacp:disabled." (3345)
- ❒ MAC address-based VLANs and static trunks. The documentation states that the ports of a MAC address-based VLAN form a community and that the assignment of a MAC address to one port in a VLAN is equivalent to assigning it to all ports. This is true except in the case where the ports of a MAC address-based VLAN encompass a static port trunk, in which case the same MAC addresses must be assigned to all the ports in the trunk. (3249)
- ❒ File upload or download. The switch's response to management instructions may be slow when you upload or download files to the file system.
- ❒ Reserved multicast traffic and port mirroring. The destination port of a port mirror may transmit duplicates of some reserved multicast traffic, such as STP BPDUs and other control packets. The duplication results from the destination mirror port transmitting both the reserved multicast traffic it receives from flooded multicast traffic and the same multicast traffic from the mirrored ports. (3055)
- ❒ Fiber optic port configuration display. The Auto-Negotiation, speed, and duplex mode settings in the menus interface for ports 23 and 24 on the AT-9424T/GB and AT-9424T/SP switches always reflect the settings of the corresponding twisted pair ports 23R and 24R. They do not reflect the current settings of an active GBIC or SFP fiber optic port. (3047)
- ❒ GVRP compatibility. To avoid possible compatibility issues with GVRP and other switches. set the GVRP Join Timer to 60 and the Leave Timer to 120.
- ❒ Spanning tree and LACP trunks. A spanning tree protocol on a switch with two or more LACP trunks uses the trunk ID number to select a trunk to place in the blocking state if the trunks form a network loop. The trunk ID number is automatically assigned by the management software when an aggregator is created. The numbering starts with 0 (zero) and increments by 1 for each new aggregator. The lower the trunk ID number, the higher the priority. For instance, a spanning tree protocol will block the ports of the trunk with the higher ID number (lower priority) if two trunks on the switch form a loop. (4261)
- ❒ Port configuration. The speed, duplex mode, and MDI/MDIX settings of a 10/100/1000Base-T twisted pair port are changed as a unit if multiple ports are configured simultaneously. The settings of the lowest numbered port are automatically copied to the other ports. For example, if you configure ports 1 to 4 simultaneously and change the MDI/MDIX setting, the speed and duplex mode settings of port 1, along with the new MDI/MDIX setting, are copied to ports 2 to 4. (1262)
- ❒ Jumbo frames loss. Frame loss on oversubscribed ports will be greater for jumbo frames (1522 bytes or larger) than for regular frames, as illustrated here:(1412, 2783, 2792)

  Regular Traffic

  64 byte size frames @ 100% wire-speed = 1,488,100 packets per second (pps):

TX Port 1 (1,488,100 pps) =>
=> Receiving (Rcv rate = 1,488,100 pps) Total Loss = 50% Port 1 / 50% Port 2
TX Port 2 (1,488,100 pps) =>

Jumbo Traffic
9000 byte size frames @ 100% wire-speed = 13,851 pps:

TX Port 1 (13,851 pps) =>
=> Receiving Total Loss (approx.) = 62.5% Port 1 / 62,5% Port 2
TX Port 2 (13,851 pps) =>

- .Xmodem downloads. The switch does not respond to echo requests or send or respond to STP BPDU packets during an Xmodem download of system software. Also, echo request responses are slowed when there is a TFTP transfer in progress and the echo requests are received within the same port group as the TFTP server. (1663, 1582)
- SFP and GBIC ports. The switch considers the fiber optic port on an optional SFP or GBIC module in the AT-9424T/GB and AT-9424T/SP switches as active even if the port is receiving a signal but has not established a valid link with the remote node. If an optional fiber optic port loses or is unable to establish a link but is receiving a signal, it remains as the active port and the switch does not activate the corresponding twisted pair port 23R or 24R. (2850)
- Web browser interface. The web browser interface works best with Microsoft Internet Explorer version 6.0 and above. Results using other versions or other web browser applications may vary.
- Enhanced stacking. The IP address 172.16.16.16 is reserved for the enhanced stacking feature. Do not assign this address to any device in the same subnet as an enhanced stack.
- Login password. The maximum length of a login password is 16 alphanumeric characters for manager accounts created through the RADIUS and TACACS+ authentication protocols and supplicant accounts for 802.1x port-based network access control. Passwords that exceed this limit will not work.
- TACACS+. The TACACS+ client software on the switch supports Password Protection Protocol (PAP), but not Challenge Handshake Authentication Protocol (CHAP) or AppleTalk Remote Access Protocol (ARAP). (1078)
- MAC addresses. You must move the cursor manually from field to field when entering an IP or MAC address in the web browser interface. The cursor does not move automatically as you enter the parts of an address. (1699, 2123)
- SNTP. The SNTP client software on the switch sends a Transmit Time Stamp with a value NULL when synchronizing with a Network Time Protocol server. This does not affect the operation of the SNTP client software. (1676)
- SFP modules and the AT-9408LC/SP Switch. Always disconnect the fiber optic cable from an SFP module in an AT-9408LC/SP Switch before removing the module. The L/A LED for the slot may remain on if you remove an SFP module while it has a link to an end node. This problem does not affect the operation of the switch or the SFP slot. The L/A LED goes off the next time you install an SFP module in the slot.
- SET STACK command. The NEWMODULEID parameter in this command has a STATIC option that is suppose to let you convert dynamic stack ID numbers into static ID numbers. This option does not work. To assign a static ID number to a switch, enter the number with the NEWMODULEID parameter (e.g., NEWMODULEID=2).

Features History

Version 3.2.0

This release added several new features to stacks of Basic Layer 3 AT-9400 Switches. The full list of features is given here. Those marked with an asterisk were new in Version 3.2.0:

- ❐ Local management
- ❐ Remote Telnet management
- ❐ Remote web browser management*
- ❐ Basic port configuration
  - — Port status (enabled or disabled)
  - — Auto-Negotiation
  - — Speed
  - — Duplex-mode
  - — Flow control and backpressure
  - — MDI or MDI-X setting
  - — Packet filtering and rate limiting
- ❐ Port statistics
- ❐ Static port trunks
- ❐ Link Aggregation Control Protocol (LACP) trunks*
- ❐ Port mirroring
- ❐ Event log
- ❐ Syslog client
- ❐ Class of Service
- ❐ Internet Group Management Protocol (IGMP) snooping*
- ❐ Spanning tree protocol (STP)
- ❐ Rapid spanning tree protocol (RSTP)
- ❐ Port-based and tagged VLANs
- ❐ Internet Protocol Version 4 packet routing with static routes* (Does not support the Routing Information Protocol.)
- ❐ Basic 802.1x port-based network access control* (Does not support MAC address-based authentication, Guest VLANs, or supplicant and VLAN associations.)

This release of the AT-S63 Management Software did not add any new features to stand-alone AT-9400 Switches. For a list of the stand-alone features, refer to the AT-S63 documentation set.

Version 3.1.0

- ❐ Support for the AT-9424T Basic Layer 3 Switch.

Version 3.0.0:

- ❐ Stacking
- ❐ Virtual Router Redundancy Protocol (VRRP)
- ❐ Ethernet Protection Switching Ring (EPSR) snooping

- ❐ Internet Protocol version 4 packet routing enhancements:
  - — Auto-summarization of routes
  - — Split horizon with poison reverse
  - — DHCP/BOOTP relay
- ❐ 802.1x port-based network access control. Added the following authentication methods:
  - — EAP-TLS (Extensible Authentication Protocol - Transport Layer Security)
  - — EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security)
  - — PEAP (Protected Extensible Authentication Protocol)

Version 2.2.0:

No new features.

Version 2.1.1:

- ❐ The number of cooling fans in the AT-9424Ts switch was reduced from four to three. The AT-S63 Management Software was updated to reflect the change.

Version 2.1.0:

- ❐ Multiple IPv4 routes with Equal Cost Multi-path (ECMP). The switch now supports ECMP and multiple routes to the same remote destination.
- ❐ Variable length subnet masks for IPv4 routing. Previously, a byte in a subnet mask for a route in the IPv4 routing table had to be 0 or 255. The switch now accepts masks of variable length.
- ❐ Multiple default routes. In the previous version, there could be only one default route for the IPv4 packet routing feature and the route was not propagated by RIP. In this version, the routing table can store and propagate multiple static and dynamic default routes.
- ❐ 802.1x authenticator ports. The maximum number of supplicants that can be logged on to an authenticator port running in the multiple operating mode has been increased from 20 clients to 320 clients. However, the maximum number of logged on clients per switch remains the same at 480 clients. (4186)

Note:
The IPv4 routing feature is not supported on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP Switches. These switches support only one routing interface for assigning the device an IP address.

Version 2.0.0:

- ❐ Internet Protocol Version 4 (IPv4) packet routing. The AT-9400 Series switch features IPv4 packet routing with routing interfaces, static routes, and the Routing Information Protocol versions 1 and 2.
- ❐ Secure Shell (SSH) protocol server. The security of the SSH server on the switch has been enhanced to prevent unauthorized management access to the switch. The AT-S63 Management Software now disables the SSH server, logs an event in the event logs with the client's IP address, and sends an SNMP trap if it detects fifty consecutive failed login attempts from an SSH client.
- ❐ Class of Service and Queue 7. The range of the maximum number of transmitted packets for the CoS weighted round robin scheduling method has been changed for Queue 7 (Q7). The

range was 1 to 15; the new range is 0 (zero) to 15. Setting Q7 to 0 gives its packets priority over packets in the other queues. No packets are transmitted from the lower priority queues so long as there are packets in Q7. (3803)

- Temperature threshold alert. The temperature threshold alert feature now has two levels. An ambient temperature of 55° to 60° Celsius for ten minutes activates the first level. The switch sends a SNMP trap and enters a warning event message in the event logs. The second level, activated if the ambient temperature exceeds 60° Celsius for five minutes, sends another SNMP trap, logs an error event message, and activates the Fault LED on the front panel.

Version 1.3.0:

- Added the following new features to 802.1x port-based network access control:
  - Guest VLANs
  - VLAN Assignment and Secure VLAN features for supporting dynamic VLAN assignments with supplicant accounts.
  - MAC address-based authentication as an alternative to 802.1x username and password authentication.
- Simplified the menu interface for managing the access control entries in the Management ACL.

Version 1.2.0:

- MLD snooping for MLDv1 and MLDv2.
- 802.1x port-based network access control supports up to 20 supplicants simultaneously on an authenticator port.
- Quality of Service has the following new actions:
  - Set Type of Service (ToS)
  - Move Type of Service to 802.1p Priority
  - Move 802.1p Priority to Type of Service
  - Send to Mirror Port
- The command line interface has new command parameters for displaying and deleting specific types of MAC addresses from the MAC address table.

Version 1.1.0:

- LACP (802.3ad)
- Policy-based QoS (Classifiers, Flow Groups, Traffic Classes, and Policies)
- Flash memory operations
- Access Control Lists (ACLs)
- Syslog support
- Password reset
- Redundant power supply information
- IGMP v3 Snooping
- New web browser interface procedures

Version 1.0.0:

❒ Auto-Negotiation (IEEE 803.3u-compliant) for speed and duplex mode

❒ Auto and manual MDI/MDI-X

❒ Flow control (IEEE 802.3x and 802.3z-compliant)

❒ Head of line blocking prevention

❒ Unicast, multicast, and broadcast rate control

❒ Port mirroring

❒ Port trunking (IEEE 802.3ad) (static link aggregation, non LACP)

❒ Port security

❒ Port statistics (RMON)

❒ 1000 static MAC addresses, 16K dynamic MAC addresses, 256 static multicast addresses, 255 dynamic MAC addresses (snooping)

❒ Spanning Tree Protocol (IEEE 802.1D)

❒ Rapid Spanning Tree Protocol (IEEE 802.1w)

❒ Multiple Spanning Tree Protocol (IEEE 802.1s)

❒ Virtual LANs (IEEE 802.1Q)

❒ Protected ports VLANs

❒ Ingress filtering

❒ GARP VLAN Registration Protocol (GVRP)-based dynamic VLANs

❒ Secure Sockets Layer (SSL) Protocol (not included in AT-S63 NE)

❒ Secure Shell (SSH) Protocol (not included in AT-S63 NE)

❒ Public Key Infrastructure (PKI) Certificates (not included in AT-S63 NE)

❒ Static and dynamic system time (SNTP client)

❒ Management VLAN

❒ Multiple VLAN modes

❒ Event log

❒ Enhanced stacking (for management)

❒ IGMP Snooping (RFC 2236)

❒ Class of Service (IEEE 802.1p-compliant)

❒ Queuing - map 802.1p to CoS queue to prioritize traffic at egress

❒ Strict priority and weighted round robin priority scheduling

❒ RRP Snooping

❒ File system

❒ SNMPv1, SNMPv2c and SNMPv3 management

❒ CLI-based configuration file

❒ Denial of Service detection

❒ 802.1x Port-based Network Access Control

❒ RADIUS accounting

- Menus, CLI, web, and SNMP interfaces
- Password protected management access
- Management access control list
- Local authentication
- RADIUS and TACACS+ authentication protocols
- Xmodem and TFTP downloads and uploads, HTTP and enhanced stacking
- Static IP configuration
- BOOTP and DHCP
- Fan and temperature information
- CPU, Flash, and RAM information
- Power supply, redundant power supply, and transceiver information

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **www.alliedtelesis.com/support/kb.aspx**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support section of the Allied Telesis web site: **www.alliedtelesis.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to the Support section on our web site at **www.alliedtelesis.com**.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**.

Management Software Updates

New releases of the management software for our managed products are available from the following Internet sites:

- Allied Telesis web site: **www.alliedtelesis.com**
- Allied Telesis FTP server: **ftp://ftp.alliedtelesis.com**

If the FTP server prompts you to log on, enter "anonymous" as the user name and your email address as the password.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.